

H04L 9/32

Recherche

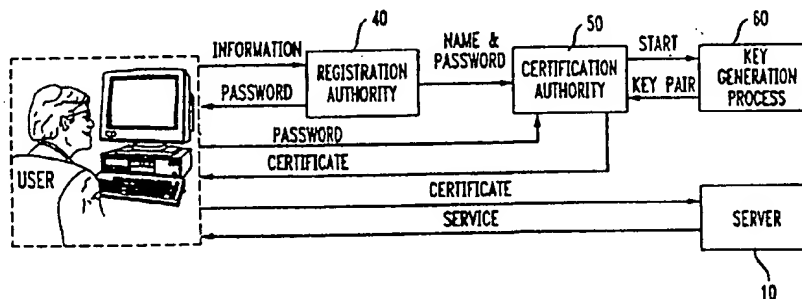
PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04L 9/32	A1	(11) International Publication Number: WO 98/39878
		(43) International Publication Date: 11 September 1998 (11.09.98)
(21) International Application Number: PCT/US98/01895		(81) Designated States: CA, JP, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).
(22) International Filing Date: 6 February 1998 (06.02.98)		Published With international search report.
(30) Priority Data: 08/812,640 7 March 1997 (07.03.97)		
(71) Applicant: AT & T CORP. [US/US]; 32 Avenue of the Americas, New York, NY 10013-2412 (US).		
(72) Inventors: HSU, Yung-Kao; 319 Arlene Terrace, Aberdeen, NJ 07747 (US). SEYMOUR, Seymour; 32 Church Street, Bound Brook, NJ 08805 (US).		
(74) Agents: DWORETSKY, Samuel, H. et al.; AT & T Corp., P.O. Box 4110, Middletown, NJ 07748 (US).		

(54) Title: AN IMPROVED CERTIFICATION PROCESS



(57) Abstract

An improved secure communication arrangement separates the tasks of identity verification and certificate issuing, which allows a disassociating of the long-term binding between Alice and her public/private key pair. This is accomplished by a registration authority issuing a password to Alice once it is satisfied of Alice's *bona fide*. Thereafter, whenever Alice wishes to communicate with Bob, she contacts a certification authority, identifies herself with the password and obtains a private key and a corresponding short-lived certificate. The certificate typically includes Alice's name and a public key in plaintext, and a signature. The signature is derived by hashing the plaintext portion of the certificate to obtain a value, and encrypting the value with the CA's private key. She then contacts Bob, submits her certificate, Bob performs the same hashing function to obtain a value, decrypts the signature with CA's public key to obtain a decrypted value, and compares the value Bob created with the decrypted value. If the two match, Bob is assured that the person submitting the certificate may be communicated with by using the public key included in the certificate.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakhstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

AN IMPROVED CERTIFICATION PROCESS

Background of the Invention

This invention relates to certifications used in connection with secure and
5 authorized communications.

In some applications, a user who wishes to obtain goods or services from
a provider is asked to authorize a charge against the user's credit card number.
In such applications, the security concern lies most heavily on the user, who
worries about the security of the transmitted information. In other applications, a
10 user may seek to obtain proprietary information from the provider, and there the
security concern lies most heavily on the provider. In the latter situation,
however, the provider is also concerned about the identity of the user.

With respect to securing communication, it is well known that secret keys
may be used to encrypt information, but that requires both parties to have a
15 secret key. Consequently, a party that communicates with many people needs to
have many different secret keys. The effort to securely distribute and manage
many secret keys was considered just too great, until public key encryption was
invented. In public key encryption, a party, say Alice, develops a pair of keys:
one is private (which the party keeps secret) and one is public (which the party
20 makes available to others). Unless her secret key is compromised, no one but
Alice can encrypt a message that can be decrypted with Alice's public key, and
no one but Alice can decrypt a message that was encrypted with Alice's public
key. Thus, public key encryption eliminates the need to securely exchange
secret keys and also eliminates the need to have and to manage many secret keys.

25 Public key encryption, however, does not eliminate concerns about the
identity of the party supplying the public key. The reason: anyone can claim to
be Alice. To remedy this problem, the notion of certification was created
whereby Bob can demand a certificate which confirms that the party is who it
claims to be. To obtain a certificate, Alice authenticates herself to a certification
30 authority (CA) in some manner that satisfies the CA. For example, the CA may

require Alice to show her driver's license, an original birth certificate, or even more. Alice is then given (or creates) a public key encryption pair, and is given a certificate that is derived by the CA from information that binds the certificate to Alice. The information may comprise, for example, Alice's name, some
5 information that further identifies Alice, and her public key. When Alice wishes to contact Bob, she submits her certificate and Bob decrypts it with CA's public key. The decrypted certificate identifies Alice and Alice's public key, and Bob is assured that a person named Alice owns a private key that corresponds to the public key which the decrypted certificate provided.

10 This certification approach still has a problem, however, in that while Alice was certified by the CA at one point, she may no longer be certified, in the sense of still being authorized to receive the information that Bob may have. To that end, the certification process is augmented, requiring Bob to check Alice's certification against a revocation list. This list is accessed by downloading a
15 revocation list at some regular intervals from a revocation list storage means.

A number of problems remain, however, with the certification approach, and which relate to the fact that the certificates are long-lived and there is a private key that is associated with the certificate. For one, it introduces a burden on the mobility of users because it requires users to carry with them their private
20 key. Of course, that represents a security risk. Another problem is that the longevity of a certificate provides an incentive to discover, or break, the private key that is associated with the public key found in the certificate. To reduce the risk to the private key, users typically increase the length of their keys, but that increases the computational burden of the applications that encrypt or decrypt the
25 communicated information. A third problem relates to the cost of managing and administering the valid and revoked certificates for large scale intranet environments.

Summary

The certification overhead problems are greatly ameliorated by
30 separating the tasks of identity verification and certificate issuing, which allows

a disassociating of the long-term binding between Alice and her public/private key pair. This is accomplished by a registration authority issuing a password to Alice once it is satisfied of Alice's *bona fide*. Thereafter, whenever Alice wishes to communicate with Bob, she contacts a certification authority, identifies herself
5 with the password and obtains a private key and a corresponding certificate. The certificate typically includes Alice's name and a public key in plaintext, and a signature. The signature is derived by hashing the plaintext portion of the certificate to obtain a value, and encrypting the value with the CA's private key. She then contacts Bob, submits her certificate, Bob performs the same hashing
10 function to obtain a value, decrypts the signature with CA's public key to obtain a decrypted value, and compares the value Bob created with the decrypted value. If the two match, Bob is assured that the person submitting the certificate may be communicated with by using the public key included in the certificate.

In accordance with these principles, the certificate that is issued to Alice
15 is short-lived, perhaps valid only for a few hours. Such short-lived certificates remove the need for a revocation list, and remove the incentive for an interloper to discover Alice's private key.

Brief Description of the Drawing

FIG. 1 is a diagram of a prior art certification process;
20 FIG. 2 is a diagram of a certification process in accordance with the principles disclosed herein; and
FIG. 3 illustrates a certificate issued by a CA on a particular day.

Detailed Description

In light of the increasing ubiquity of Internet and Intranet transactions
25 and the awareness that these mediums are fairly insecure, the information technology industry is seeking solutions to the security concerns of users, and the current thrust is to use public key cryptography-based technologies such as the ITU X.509 Digital Certificate, and Secured Socket Layer protocol. Both Netscape and Microsoft, for example, use this technology to support secured
30 sessions between a client and a server.

FIG. 1 presents one embodiment of a prior art certification process, describing a process whereby Alice obtains a certificate for herself, and whereby Bill employs his certificate to communicate with an application that resides on application server 10. To obtain a certificate, Alice communicates with a
5 certification authority (CA) 20 in a secure manner. The certification authority may be a designated department of Alice's employer, or it may be a trusted commercial concern (e.g., the provider of telecommunication services). The secure method of communication may be the Secured Socket Layer protocol, or it may be an "in person" interaction. During this secure communication, Alice
10 provides CA 20 with whatever information the CA requires and when Alice meets the CA's criteria, CA 20 provides Alice with a certificate which includes a date of issue, a public key, a signature, and a private key that corresponds to the public key pair. The signature is derived by passing the other information through a hashing function and encrypting the resulting value with the private
15 key of the certification authority.

The certificate is typically long-lived -- on the order of months -- because its primary purpose is to vouch for Alice. More specifically, its purpose is to vouch for the fact that secure communication can be sent to Alice by encrypting information with the public key included in the certificate. The certification is
20 not permanent because, to maintain a high level of confidence in the security of communication, it is desirable to change from time to time Alice's public/private key pair. In addition to the natural expiration of the certificate, there needs to be a means for revoking a certificate when, for example, Alice's private key is compromised. Once such means are included, it can also be viewed as a means
25 to revoke a certificate for reasons other than a compromise of the private key, such as when company X no longer wishes Alice to have the capability to access company X resources.

Thus, the FIG. 1 arrangement includes a revocation list processor 30 which stores certificates that are no longer valid. Since more and more
30 certificates become invalid with time, the number of certificates stored by

processor 30 could continually increase, unless a bound is effected. Such a bound dovetails with the notion that certificates expire naturally after some long but finite life (as indicated above, typically a month or more; e.g., 1, 2, 6, 24 months). This allows processor 30 to discard from its memory those certificates
5 that were previously revoked and are now naturally expired.

When Bill wishes to access an application on application server 10 (e.g., via the Internet), he submits to server 10 a certificate which he previously received from CA 20. Application 10 hashes the plaintext portion of the received certificate to obtain a value, and also decrypts the signature portion of
10 the received certificate with CA 20's public key. If the value obtained from the hashing function corresponds to the value obtained from the decryption process, then application 10 concludes that the certification is valid; that is, that the person who is named in the certificate is the person who has a private key that corresponds to the public key which is included in the certificate.

15 It should be easily appreciated that the efforts of creating certificates, maintaining a list of revoked certificates, and engaging in the communication associated with confirming certificates present key management problems. The problem also extends to the protection of private keys, user mobility, and general operation and administration.

20 It is believed that the root cause of many of the key management problems can be traced to the long-lived nature of the certificates. When a certificate is long-lived, the possibility of it becoming invalid increases with time due to unforeseeable and/or uncontrollable events, such as compromise of the employee's private key, the employee leaving the company or leaving the project
25 that requires access authorization, etc. Long-lived certificates are also more likely to be compromised because they are almost certainly going to be stored on the hard drive of a user's computer and, sometimes, access to the computer is open. Moreover, there is more incentive for an interloper to expend the effort to compromise the private key.

FIG. 2 presents one embodiment of an improved process which eliminates the need for application server 10 to contact a revocation list processor, and which finely controls the authorization aspect of certificates.

A word about the *authorization* aspect of certificates. Including Alice's
5 name in the certificate is a form of an authorization check, in the sense that information is provided to application server 10 to definitively identify the party that is accessing the application server. However, there is no cryptographic reason to include Alice's name in the certificate. Indeed, situations often arise where an application server is not really interested in knowing who the party is
10 but only in some attribute of the party (such as, "is the party credit worthy?"). A classic example is when a person uses a credit card and the merchant is merely interested in getting paid. On the other side of the ledger, however, there are instances where knowing the certificate is valid is insufficient. The fact that the person named in the certificate, such as Bill, can be sent information in a secured
15 manner does not necessarily dispose of the question whether application server 10 should in fact grant Bill access.

In the prior art, the authorization issue is addressed in the CA, at least in part. That is, by granting a certificate the CA authorizes at least some service-providing entities, such as application server 10, to proceed. However, there
20 may be other application servers that do not wish to convey information or to provide a service unless Bill belongs to a particular class (e.g., an employee). Typically, the CA is in the best position to ascertain whether Bill should be authorized and, when that is the case, the granting of a certificate by the CA is conditioned on Bill presenting evidence to the CA that Bill belongs to the subject
25 class. Alas, this introduces another time sensitivity to the certificate granted by the CA because while Bill may belong to the subject class when he requested a certificate, he may no longer belong to the subject class when he uses the certificate. That means that the reliance of prior art systems on the revocation list (30) is higher.

In contradistinction to the prior art, in the FIG. 2 arrangement the authorization issue can be shared between the CA and the application server, as appropriate, and there is no reliance on a revocation list whatsoever.

In accordance with the FIG. 2 arrangement, Alice is accepted into "the fold" through a contact with registration authority (RA) 40 over a secured channel. During this contact Alice submits whatever proofs and information RA 40 requires to satisfy itself of Alice's *bona fide*, and once RA 40 is satisfied, it provides Alice with a public key of certification agent (CA) 50, and it issues Alice a password. RA 40 then informs CA 50 of Alice's password and
10 authorization information, either over a secured channel or by encrypting the information with CA 50's public key.

Thereafter, whenever Alice needs a certificate, she contacts CA 50, identifies herself with the password (or a hardware token that increases the level of security), and perhaps submits to CA 50 some other information, such as the
15 purpose(s) to which Alice wishes to apply the certificate. To protect Alice's password, the communication from Alice can be over a secured channel, or it can be encrypted with CA 50's public key. Once CA 50 has the request, it can determine whether the password is valid. If so, CA 50 proceeds to ascertain whether the purpose for which the certificate is requested is an authorized
20 purpose. If it is not, the certificate is refused. Otherwise, CA 50 obtains a public/private key pair (e.g., process 60) for Alice, and proceeds to construct a certificate. Illustratively, the certificate comprises an expiration time, Alice's public key, Alice's name, Alice's private key, the purpose for which the certificate was requested or some other authorization code, the name of the
25 certification authority, a serial number (so that the CA can keep track of what certificates it issued and to whom), and a signature. The signature is obtained, as in the prior art, by hashing the plaintext information in the certificate to obtain a value and encrypting that value with the private key of CA 50.

Significantly, as stated above, the FIG. 2 arrangement does not require an
30 application server to download or to otherwise access or consult a revocation list.

Rather, the certificate provides all of the information that an application server 10 needs to determine that a) the certificate is valid, and b) use of the certificate is still authorized. In accordance with the principles disclosed herein this is achieved, at least in part, by having certificates that are short-lived. That is, the
5 expiration time of certificates created by the FIG. 2 arrangement is less than one month, and typically much less than one month. In fact, the typical certificate created by the FIG. 2 arrangement may be good for only one day and perhaps for even less than one day. For example, the expiration time of the certificate may include merely a date, a date with an implicit time (e.g., the end of a business
10 day), or it may include a date and an explicit time (e.g., 3/18/97-16:00).

In a further improvement which generically tightens authorizations, a certificate created by the FIG. 2 arrangement may include a "number of uses" limitation. The number of uses limitation may be explicit, by including a number in the certificate, or it may be implicit. For example, the FIG. 2
15 arrangement may be set so that each certificate is honored by any application server 3 times, or a certificate is honored by one application server 10 times, and by another application server only once.

The fields that correspond to the expiration time and the number of uses are but two of the mechanisms to control access. A third mechanism for
20 controlling access is embodied in the information regarding the purpose for which the certificate was requested, or the purpose for which the certificate is issued (the two may be synonymous, but not necessarily so). The fact that CA 50 grants a certificate and includes information that allows an application server to decide whether to provide access effectively transfers some authorization
25 control from CA 50 to the application servers to which the certificates are offered. This may be advisable because CA 50 may not have its authorization profiles up to date, or for other reasons it is not advisable to keep all authorization data centrally. Of course, there are some clear advantages to keeping at least some authorization control centrally in CA 50. First, at least
30 some authorization information is more likely to be known to CA 50; second,

centralization of such information is a more efficient way to maintain control over the myriad application servers that an enterprise might have; and third, centralization reduces the risk of information being compromised. Further, when a request for a certificate (for a particular purpose) does not pass muster under the authorization information available in CA 50, the grant of a certificate is simply refused.

For the certificate described above, which includes Alice's private key, the communication of the certificate from CA 50 to Alice must be over a secured channel. This requirement, however, may be dispensed with, and Alice may be offered an additional measure of security by allowing Alice to generate her own key pair. In such an arrangement, Alice creates a public/private key pair, provides CA 50 with her public key in addition to the other required information, and CA 50 responds with a certificate. No private key information is communicated.

Stripped to the minimum, the goals of a certificate communicated by CA 50 to Alice are satisfied by merely associating a public key with a private key that Alice has, by including information which indicates that the certificate is not stale or expired, and by providing a mechanism to assure the recipient of a certificate that CA 50 vouches for whatever information is communicated by the certificate to the application server. This mechanism is a "stamping" of the certificate's information with the private key of CA. The stamping can be effected by collecting the information of the certificate, encrypting the collected information with the private key of CA 50, and presenting the encrypted result as the certificate. Alternatively, the stamping can be effected with a signature created in accordance with the above-described prior art techniques.

The stamping by means of a signature is more compact than the encryption of the entire set of information that is contained in the certificate, but an even more shorter transmission from CA 50 to Alice is achieved by simply not including some of the information that Alice already has. For example, Alice already knows her name, her public key, and the purpose for which she

wishes to use the certificate (as she communicated that purpose to CA 50). Alice may even know that the certificate she gets will be valid only for the current day only (e.g., the certification will expire at the "end of business" of the day the certificate was requested). In such a case, CA 50 might dispense with sending
5 the unnecessary information and rather send only the information that Alice does not have, such as the signature, perhaps an authorization code, and the like (e.g., the public key of application server 10 -- which is really not part of the certificate). Effectively, CA 50 limits itself to sending only the certificate core, allowing Alice to construct the rest of the certificate. Of course, whatever Alice
10 appends to the certificate core must be known to CA 50 or must have been communicated to CA 50 for inclusion in the information that is "stamped."

One additional piece of information that is included in the above-described certificate and which might not be needed is the identity of the certification authority. If that is known and understood by whatever application
15 servers are accessed by Alice, the certificate need not include that data. This, of course, can be a variable which depends on the information provided by Alice to CA 50. For example, when Alice wants to communicate with a server that belongs to her employer, the certificate will not include the CA's identity. When Alice wishes to communicate with, say, the U.S. Patent and Trademark Office
20 (PTO), the certificate will include the CA's identity.

With a certificate at hand, Alice contacts application server 10 (e.g., via the Internet) and submits her certificate to the server. Server 10 verifies the certificate with the public key of CA 50 and, if appropriate (based on the information contained in the certificate), concludes that communication with
25 Alice can proceed, determines the level of service that it will provide to Alice, and knows that it needs to respond to Alice by using Alice's public key for encryption (while Alice may use the public key of application server 10). Since public key encryption is computationally more intensive than a symmetric secret key, the first and perhaps the only communication that server 10 might engage in
30 by using Alice's public key is a transmission of a secret key to Alice. Since only

Alice has the appropriate private key that corresponds to the public key, only Alice can decrypt and thereby utilize the secret key provided by application server 10. Subsequent session communications between Alice and server 10 can then take place using the secret key. While the same secret key could be used in
5 later sessions between Alice and application server 10, there is a clear security advantage in using a different secret key with each session.

To summarize, the arrangements of FIG. 1 and FIG. 2 contemplate using secure communications between users such as Alice and Authorities 20 and 40, and insecure communications between the users and application server 10 (and
10 also CA 50). What the FIG. 2 arrangement saves is the need for a revocation list and the need for server 10 to communicate with a revocation list processor 30. Correspondingly, the certificate created for the FIG. 2 arrangement differs in character from the prior art certificates obtained for the FIG. 1 arrangement. If the latter is likened to a driver's license because it is long-lived, then the former
15 can be likened to a subway token or to a bus ticket because it is short-lived. Also, the certificate created for the FIG. 2 arrangement is more like an authorization to an application server than a confirmation of a party's identity.

The advantages accruing from the FIG. 2 arrangement can be appreciated by sketching out a typical arrangement. In such an arrangement, Alice is an
20 employee of company X and is stationed at location x1. Company X has many other locations and many other employees. At one of its locations, company X maintains (for security and efficiency reasons as discussed above) an overall database of its employees and processing capabilities to implement the registration authority. Company X would most likely have a single registration
25 authority because the communication burden on the registration authority is fairly light. When Alice needs a password, which is chosen to be relatively long-lived (e.g., significantly more than one week), she contacts the registration authority in a secure manner, as discussed above. Since such communication occurs relatively infrequently (only when Alice is first qualified and thereafter

only when a new password is needed), the burden on Alice and on the infrastructure of communication into RA 40 is not great.

In contrast to the single RA 40, company X may have a certification authority 50 in each of its locations. Each of the CA 50s is supplied with
5 information from RA 40 whenever a new password is issued to an employee that a particular CA 50 is charged with servicing, or when new authorizations take effect. This communication is either over a secured channel or is encrypted with the public key of CA 50, and it, too, is infrequent.

When Alice wishes to obtain a certificate, she contacts her local CA 50.
10 Again, this contact must use a secure channel of communication or be encrypted with the public key of CA 50. When the desired certificate is for contacting an application server of company X, the certificate need not identify the CA, since that is understood.

Having obtained a certificate, Alice can access any resource of company
15 X throughout its far flung reaches and can securely communicate over a relatively insecure medium such as Internet. These resources, which may be a single computer that contains information or performs computations, or whole networks of computers that, perhaps, control operations for company X, belong to company X and it is a simple matter to have them installed with knowledge of
20 the public key of company X. Each application that is accessed by Alice on such a remote resource needs only to execute a module that decrypts a certificate and monitors a "hand shaking" protocol with Alice (such as sending Alice a secret key and receiving a confirmatory response from Alice). No communication by this module with the "outside world" needs to take place and that, of course, is a
25 significant advantage.

Alice might be restricted to only some of the resources that belong to company X, and the restrictions may be based on Alice's status. For example, because Alice is an employee of company X she may be entitled to access information in the company's library; by virtue of being on the team of project
30 Y, Alice may be permitted to access files in a certain server; and by virtue of

being the administrator of the company's payroll computer, Alice may be permitted to "bring down" the computer for maintenance. Clearly, in accordance with the principles disclosed herein, Alice can obtain a number of certificates, and each certificate specifies the particular authorization that is granted.

- 5 Alternatively, a single code might suffice. When application server 10 receives a certificate that includes a number of uses limitation, it accesses a count of the number of times the certificate had been used, increments the count, and when the count exceeds the maximum number for which the certificate is good, service is refused.

- 10 Of course, this approach can also be used in connection with a resource that is owned by other than company X. For example, a company such as AT&T can provide its public key to another entity, say U.S. PTO, and provide a certificate to each of its intellectual property attorneys. The PTO can then receive applications, amendments, etc. over the Internet with assurance that the
15 attorney does operate on behalf of AT&T. Illustratively, a certificate that precedes an electronic filing of a patent application with the PTO is shown in FIG. 3.

- The notion of a transfer that is common in subway tokens can also be implemented in the FIG. 2 certificates. For example, a particular server 10 may
20 decide to "hand off" Alice to another server. It can issue its own certificate to vouch for Alice to that other server and offer Alice's certificate so that the other server would get Alice's public key.

Claims:

1. A method comprising the steps of:
a certification authority (50) interacting with a user to receive
5 information from the user;
developing a certificate core (FIG. 3) that comprises a stamping of first
data with a private key of the certification authority (CA-PrKey), which first data
comprises a public key of the user and a short-lived expiration time of the
certificate, and
10 delivering the certificate core to the user to be used at least as part of the
certificate.
2. The method of claim 1 where the expiration time is less than one
month from the date the certificate is issued.
15
3. The method of claim 1 where the expiration date is the day after the
date the certificate is issued.
4. The method of claim 1 where the expiration date explicitly includes
20 the time of day.
5. The method of claim 1 further comprising the step of employing at
least a part of the certificate core as a certificate or appending information to at
least a part of the certificate core to form a certificate.
25
6. The method of claim 5 where a portion of the certificate core is not
used as part of the certificate.
7. The method of claim 5 where the appending of information to form a
30 certificate is carried out by the certification authority.

8. The method of claim 5 where the appending of information to form a certificate is carried out by the user.

5 9. The method of claim 1 where the stamping is an encryption with the CA-PrKey of the first data.

10 10. The method of claim 9 where the first data also includes one or more from the set containing identity of the certification authority, name of a user to whom the certificate is intended to be delivered, other information about the user, a field that identifies the certificate to the certification authority, a service for which the certificate is valid, a purpose for which the certificate is valid, an authorization code, a server for which the certificate is intended, and a number of uses of the certificate in a server.

15

11. The method of claim 10 where the decision whether to include the identity of the certification authority is based on information provided by the user in the step of interacting.

20

12. The method of claim 9 where the first data further comprises information provided by the user, or information provided by the certification authority, or both.

25 13. The method of claim 1 where the stamping is an encryption with CA-PrKey of a value which is derived from a hashing of the first data, and the certificate core further comprises second data which comprises the public key of the user and the short-lived expiration time of the certificate.

30 14. The method of claim 13 where the appending of information to form a certificate is carried out by the certification authority.

15. The method of claim 13 where the appending of information to form a certificate is carried out by the user.

5 16. The method of claim 13 where the second data further comprises one or more from a set comprising the name of the user, other information about the user, service for which the certificate is intended, service for which the certificate is valid, authorization code, expiration time of the certificate, or a number of uses of the certificate in a server.

10

17. The method of claim 16 where the information appended to the certificate core to form a certificate is included in the first data.

15 18. The method of claim 13 where the public key of the user is either provided by the user or by the certification authority.

19. The method of claim 13 where the second data further comprises information provided by the user, or information provided by the certification authority, or both.

20

20. The method of claim 13 where the information provided by the certification authority in the second data includes a public key that is associated with the private key of the user.

25 21. The method of claim 13 where the first data is identical to the second data.

22. A method carried out in a processor (10) for responding to a connection request comprising the steps of:

30 receiving a certificate that includes an expiration time;

determining the certificate's *bona fide*;
refusing to continue the connection either when the certificate is not *bona fide* or when the expiration time has passed; and
carrying on the connection with aid from a public key contained in the
5 certificate, without reference to information regarding revocation of certificates
downloaded to the processor, when the expiration time of the certificate has not
yet arrived.

23. The method of claim 22 where the step of determining the
10 certificate's *bona fide* comprises:
processing at least some plaintext information included in the certificate
to obtain a value;
encrypting the value with a public key of a known certification authority
to obtain a signature;
15 comparing the obtained signature with a signature contained in the
certificate; and
accepting a first field of information contained in the certificate as a *bona fide*
expiration time and a second field of information contained in the certificate
as a *bona fide* user public key.

20
24. The method of claim 23 where the first field is either plaintext,
encrypted with a private key of the certification authority that corresponds to the
public key of the certification authority, or encrypted with a user private key that
corresponds to the user public key.

25
25. The method of claim 23 where the second field is either plaintext or
encrypted with a private key of the certification authority that corresponds to the
public key of the certification authority.

26. The method of claim 22 where the step of determining the certificate's *bona fide* comprises:

obtaining a public key of a certification authority;
decrypting the certificate; and

5 accepting a first field of information contained in the certificate as a *bona fide* expiration time and a second field of information contained in the certificate as a *bona fide* user public key.

27. The method of claim 22 further comprising, prior to the step of
10 refusing the connection,

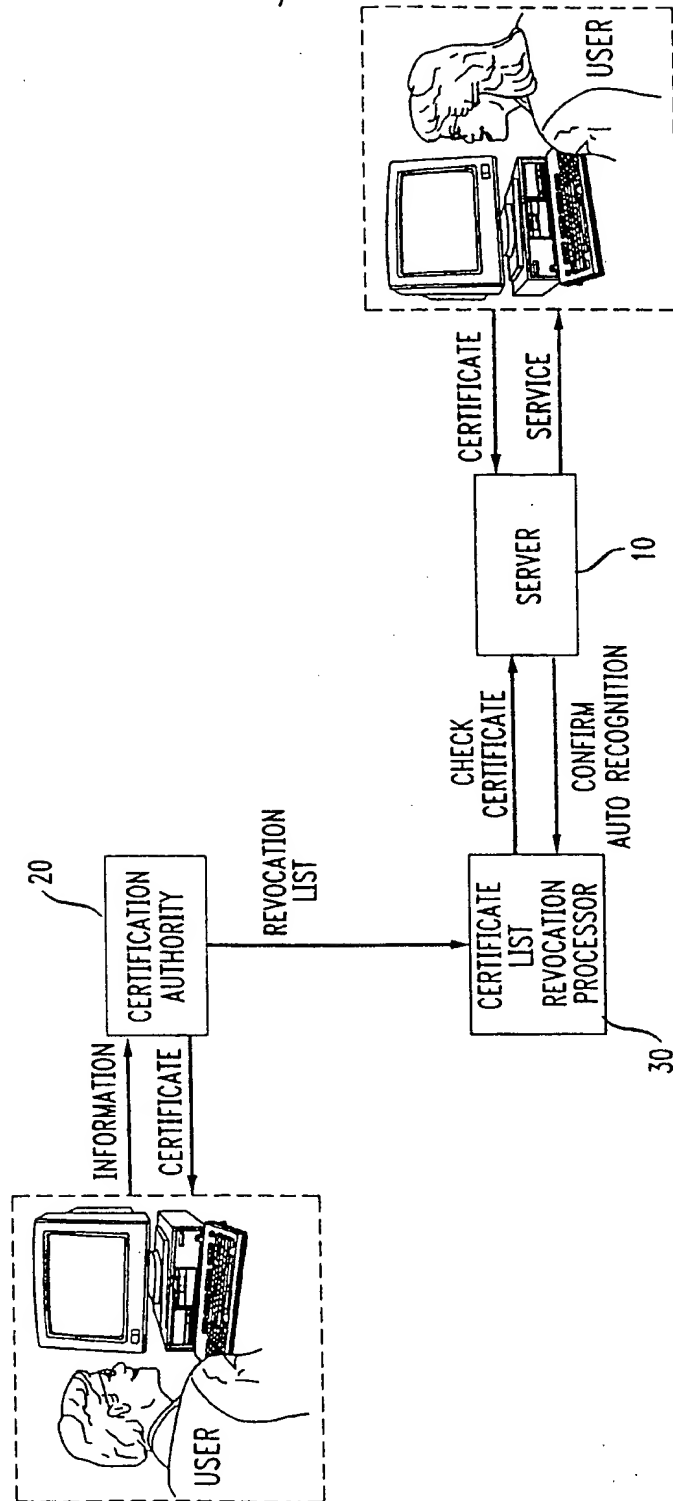
a step of determining from other information contained in the certificate, and without reference to information received by the processor with respect to the received certificate, whether the processor should respond to the connection request,

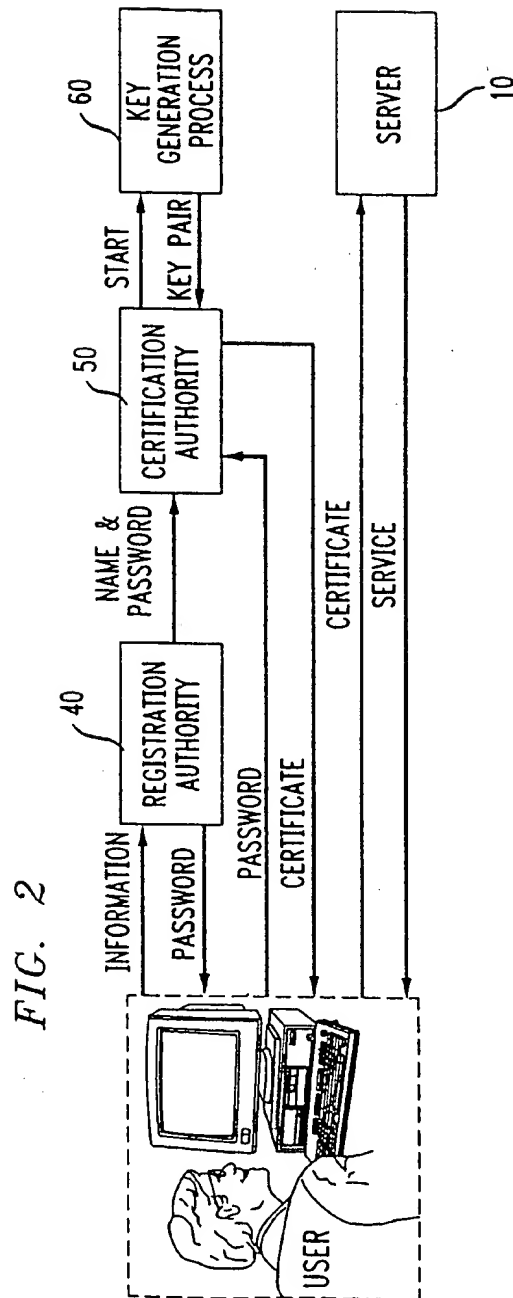
15 where the step of refusing to refuse to continue the connection is executed also when the step of determining concludes that communication should be refused.

28. The method of claim 22 where the information contained in the
20 certificate which is utilized in the step of determining is a purpose for which the certificate is to be employed, a service for which the certificate is employed, an application server identity, or number of uses information.

1/3

FIG. 1





3/3

FIG. 3

SERIAL NO.	101
DATE	03/01/97-18:00
NAME	ALICE JONES
ATTRIBUTE	MEMBER OF TEAM XY12
KEY	ser!23V*990)qdv!3=%JKwq493
USES	3
CA	
CA KEY	
SERVICE	LIBRARY ACCESS
AUTHORIZATION CODE	523
PURPOSE	ACCESS DATABASES(NO MODIFICATIONS)
SIGNATURE	ro9els&<2ksLQ+1@P[[sjd2Jd

INTERNATIONAL SEARCH REPORT

Int. Patent Application No.
PCT/US 98/01895

A. CLASSIFICATION OF SUBJECT MATTER

IPC 6 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	TAHER ELGAMAL, JEFF TREUHART, FRANK CHEN: "Securing Communications on the Intranet and over the Internet" NETSCAPE COMMUNICATIONS CORPORATION, July 1996, XP002066298 Available from Internet: <URL: http://www.go-digital.net/whitepapers/ securecomm.html> 27 May 1998. see page 3, line 35 - page 5, last line see page 8 see page 10, line 20 - page 11, line 35 see page 12, last paragraph - page 13, line 34	1,5-7,9, 12
A	---	13,22

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

28 May 1998

Date of mailing of the international search report

16/06/1998

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 eponet,
Fax: (+31-70) 340-3016

Authorized officer

Gautier, L

INTERNATIONAL SEARCH REPORT

In tional Application No
PCT/US 98/01895

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>PURSER M: "COSINE SUB-PROJECT P8: SECURITY SERVICES" COMPUTER NETWORKS AND ISDN SYSTEMS, vol. 25, no. 4 / 05, 1 November 1992, AMSTERDAM, NL, pages 476-482, XP000306614 see page 478, right-hand column, line 4 - page 480, left-hand column, line 2 see page 480, left-hand column, line 4 - right-hand column, line 20 see figures 4-6</p> <p>---</p>	1-5,9, 13,22
A	<p>US 5 261 002 A (PERLMAN RADIA J ET AL) 9 November 1993 see abstract see column 2, line 28 - line 68 see column 4, line 5 - line 9 see column 6, line 10 - line 35 see claim 1 see figure 2</p> <p>-----</p>	1-5,9,13

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 98/01895

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5261002 A	09-11-1993	NONE	